UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,415	08/31/2000	Osamu Kobayashi	GNSS-0019	4253

22434 7590 06/28/2004

BEYER WEAVER & THOMAS LLP
P.O. BOX 778
BERKELEY, CA 94704-0778

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/652,415	KOBAYASHI ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-12 and 18-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-12 and 18-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 3-12 and 18-26 are presented for examination.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3-4, 6-7, 9, 11-12, 18-23, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narui et al., (U.S. Patent No. 6,313,813 and Narui hereinafter), in view of Shimizu et al., (U.S. Patent No. 6,085,623 and Shimizu hereinafter), in further view of Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter).

Regarding claim 12, Narui discloses display circuit for use in a display unit, said display circuit comprising:

a data decryption circuit receiving said plurality of digital data elements and generating said plurality of pixel data elements, wherein said image is generated on a display screen based on said plurality of pixel data elements, and wherein said display signal is received according to TMDS format (Col. 4, lines 30-67).

Narui does not expressly disclose encryption protocol and encrypted key.

However, Shimizu discloses:

a non-volatile memory (i.e., storage device 12) storing an encrypted key, wherein said encrypted key is generated from an unencrypted key according to an encryption protocol (Col. 7, lines 4-55); and

Shimizu does not expressly disclose and integrated circuit coupled to a non-volatile memory.

However, Ashe discloses an integrated circuit (i.e., DSP) coupled to said non-volatile memory (i.e., EPROM), said integrated circuit receiving said key in encrypted form (i.e., Zi, encrypted Kc) and decrypting said key to generate a decrypted key (i.e., Kc, decrypted Zi), said integrated circuit using said decrypted key (i.e., reading the encrypted program Y with the customer decryption algorithm module 23) wherein said integrated circuit comprises a key encryption circuit receiving said unencrypted key, said key encryption circuit generating said encrypted key from said unencrypted key according to said encryption protocol, a key decryption circuit receiving said encrypted key and generating said decrypted key according to said encryption protocol, a receiver adapted for receiving a plurality of digital data elements encoded in a display signal, wherein said digital data elements represent a plurality of pixel data elements in an encrypted form, said plurality of pixel data elements representing an image (Col. 2, lines 65-67 and Col. 3, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Narui with the teachings of Shimizu because it would allow to include a non-volatile memory storing an encrypted

key with the motivation to safely store personal data of users and to assure safety of highly confidential data shared by the plurality of users (Shimizu, Col. 1, lines 55-60), and to modify the combined teachings of Narui and Shimizu with the teachings of Ashe because it would allow to include an integrated processing unit such as a Digital Signal Processor (DSP), that has both the proprietor's unique algorithm (i.e., unencrypted key), master algorithm (i.e., encryption protocol), and master key (i.e., the key to encrypt the unencrypted key) with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10).

Regarding claim 3, Narui or Shimizu does not expressly disclose wherein said unencrypted key comprises an authentication key and said using comprises authenticating a source of data.

However, Ashe discloses wherein said unencrypted key comprises an authentication key (i.e., Kc, decrypted Zi) and said using comprises authenticating a source of data (i.e., verification that the entered key is the same as the encrypted key and allowing card holder to conduct transaction and obtaining cash via dispenser 26)(Col. 3, lines 15-38 and Col. 4, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Narui and Shimizu with the teachings of Ashe because it would allow to include wherein said unencrypted key comprises an authentication key and said using comprises authenticating a source of data with the motivation to allow a machine such as a cash machine having a

microprocessor mounted within it to read the memory and verify that the key card holder enters is the same as the encrypted key and allow the card holder to conduct transaction (Ashe, Col. 3, lines 15-36).

Regarding claim 4, Narui does not expressly disclose wherein said unencrypted key comprises a decryption key and said using comprises decrypting data.

However, Shimizu discloses wherein said unencrypted key (i.e., temporary key generated by the random number generator 3) comprises a decryption key and said using comprises decrypting data (i.e., decrypting device uses the extracted temporary key and decrypts the body portion 8)(Col. 8, lines 7-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Narui with the teachings of Shimizu because it would allow to include wherein said unencrypted key comprises a decryption key and said using comprises decrypting data with the motivation to assure safety of highly confidential data shared by the plurality of users (Shimizu, Col. 1, lines 55-60).

Regarding claim 6, Narui discloses wherein said display unit comprises an analog display unit (Col. 1, lines 22-51).

Regarding claim 7, Narui discloses wherein said display unit comprises a digital display unit (i.e., The LCD monitor 16 includes an A/D converter 18 that converts the received analog signals into digital signals)(Col. 1, lines 22-51).

Regarding claim 9, Narui or Shimizu does not expressly disclose wherein when a source of data is authenticated, wherein said authenticating is performed using said unencrypted key based on data sent and received on a path connected to said display unit.

However, Ashe discloses wherein when a source of data is authenticated (i.e., the contractor providing cash such as a bank), wherein said authenticating is performed using said unencrypted key based on data sent and received on a path connected to said display unit (i.e., the user enters PIN via the keypad and it is verified that the entered PIN is the same as the decrypted key and allow the card holder to conduct transactions and obtain cash via dispenser)(Col. 3, lines 15-38 and Col. 4, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Narui and Shimizu with the teachings of Ashe because it would allow to include wherein said authenticating is performed using said unencrypted key based on data sent and received on a path connected to said display unit with the motivation to allow a machine such as a cash machine having a microprocessor mounted within it to read the memory and verify that

the key card holder enters is the same as the encrypted key and allow the card holder to conduct transaction (Ashe, Col. 3, lines 15-36).

Regarding claim 11, Narui does not expressly disclose further comprising a master block external to said display unit that sends said unencrypted key, wherein when said encrypted key is sent to said master block, said master block stores said encrypted key in said non-volatile memory.

However, Shimizu discloses wherein a master block external to said display unit sends said unencrypted key (i.e., the temporary key generated by the random number generator is transferred to and encrypted in the encrypting device 10 of IC card 5), said method further comprising sending said encrypted key to said master block, wherein said mater block stores said encrypted key in said non-volatile memory (i.e., storage device 12)(Col. 7, lines 10-27).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Narui with the teachings of Shimizu because it would allow to include a master block external to said display unit that sends said unencrypted key, wherein when said encrypted key is sent to said master block, said master block stores said encrypted key in said non-volatile memory with the motivation to assure safety of highly confidential data shared by the plurality of users (Shimizu, Col. 1, lines 55-60).

Regarding claim 18, Narui discloses an integrated circuit, comprising:

a receiver adapted to receive a plurality of digital data elements encoded in a display signal that is received according to TMDS format and that represents a plurality of pixel data elements in an encrypted form, wherein said plurality of pixel data elements represents an image that is generated on a display screen based on said plurality of pixel data element (Col. 2, lines 62-67 and Col. 3, lines 1-67 and Col. 4, lines 30-67).

Narui does not expressly disclose receiving said unencrypted key in said display unit.

However, Shimizu discloses a key encryption circuit adapted to receive an unencrypted key and generating an encrypted key from said unencrypted key according to an encryption protocol (i.e., the encrypting device 10 encrypts the transferred temporary key using a master key stored in a master key memory 9)(Col. 7, lines 13-22).

Narui or Shimizu does not expressly disclose decrypting and using the unencrypted key in the same integrated circuit.

However, Ashe discloses:

a data decryption circuit adapted to receive said plurality of digital data elements and generate said plurality of pixel data elements, and a key decryption circuit adapted to receive said encrypted key (i.e., Zi, the encrypted Kc) and generate said decrypted key according to said encryption protocol (i.e., after the key Kc is deciphered, the DSP reads the encrypted program y with the customer decryption algorithm module 23)(Col. 2, lines 65-67 and Col. 3, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Narui with the teachings of Shimizu because it would allow to include a non-volatile memory storing an encrypted key with the motivation to safely store personal data of users and to assure safety of highly confidential data shared by the plurality of users (Shimizu, Col. 1, lines 55-60), and to modify the combined teachings of Narui and Shimizu with the teachings of Ashe because it would allow to include an integrated processing unit such as a Digital Signal Processor (DSP), that has both the proprietor's unique algorithm (i.e., unencrypted key), master algorithm (i.e., encryption protocol), and master key (i.e., the key to encrypt the unencrypted key) with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10).

Regarding claim 19, Narui or Shimizu does not expressly disclose wherein the integrated circuit is coupled to a non-volatile memory suitable for storing the encrypted key.

However, Ashe discloses an integrated circuit (i.e., DSP) coupled to said non-volatile memory (i.e., EPROM)(i.e., reading the encrypted program Y with the customer decryption algorithm module 23)(Col. 2, lines 65-67 and Col. 3, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Narui and Shimizu with the teachings of Ashe because it would allow to include an integrated processing unit such as a Digital Signal Processor (DSP), that has both the proprietor's unique

algorithm (i.e., unencrypted key), master algorithm (i.e., encryption protocol), and master key (i.e., the key to encrypt the unencrypted key) with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10).

Regarding claim 20, Narui or Shimizu does not expressly disclose further comprising:

a memory adapted to receive said encrypted key, a port coupled to said memory, said port receiving said encrypted key from said memory and sending said encrypted key to a master block adapted to store said encrypted key in said non-volatile memory.

However, Ashe discloses wherein said integrated circuit further comprises: a memory receiving said encrypted key (i.e., memory 11); and a port coupled to said memory, said port receiving said encrypted key (i.e., Zi, the encrypted Kc) from said memory and sending said encrypted key to a master block (i.e., DSP), wherein said master block stores said encrypted key in said non-volatile memory (i.e., EPROM 11)(Col. 2, lines 49-67 and Col. 3, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Narui and Shimizu with the teachings of Ashe to include a non-volatile memory such as EPROM that both receives and stores the encrypted key until it is needed with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10).

Regarding claim 21, Narui discloses wherein the integrated circuit is coupled to a display unit (Col. 1, lines 22-51).

Regarding claim 22, Narui discloses where said display unit is a digital display unit (Col. 1, lines 22-51).

Regarding claim 23, Narui discloses wherein said display unit is an analog display unit (Col. 1, lines 22-51).

Regarding claim 25, Narui does not expressly disclose further comprising: storing an encrypted key generated from an unencrypted key according to an encryption protocol in a non-volatile memory.

However, Shimizu discloses:

a non-volatile memory (i.e., storage device 12) storing an encrypted key, wherein said encrypted key is generated from an unencrypted key according to an encryption protocol (Col. 7, lines 4-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Narui with the teachings of Shimizu because it would allow to include storing an encrypted key generated from an unencrypted key according to an encryption protocol in a non-volatile memory with the motivation to assure safety of highly confidential data shared by the plurality of users (Shimizu, Col. 1, lines 55-60).

Claims 24 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narui et al., (U.S. Patent No. 6,313,813 and Narui hereinafter), in view of Shimizu et al., (U.S. Patent No. 6,085,623 and Shimizu hereinafter), in further view of Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter, in further view of, Muratani et al., (U.S. Patent No. 6,061,451 and Muratani hereinafter).

Regarding claim 24, Narui discloses comprising:

receiving a plurality of digital data elements encoded in a display signal wherein said display signal is received according to TMDS format, and wherein said digital data elements represent a plurality of pixel data elements in an encrypted form that represent an image (Col. 2, lines 62-67 and Col. 3, lines 1-67 and Col. 4, lines 30-67).

Narui does not expressly disclose receiving said unencrypted key in said display unit.

However, Shimizu discloses receiving an unencrypted key generating said encrypted key from said unencrypted key according to an encryption protocol (i.e., the encrypting device 10 encrypts the transferred temporary key using a master key stored in a master key memory 9), and generating a decrypted key by decrypting the encrypted key according to said encryption protocol (i.e., the decrypting device 20 decrypts the input data using the master key stored in the master key memory 9,

thereby extracting the original temporary key used in encryption)(Col. 7, lines 13-67 and Col. 8, lines 1-20);

Narui or Shimizu does not expressly disclose receiving a display signal in encrypted format.

However, Muratani discloses further comprising decrypting said encrypted plurality of digital data elements, generating said plurality of pixel data elements based upon said decrypted plurality of digital data elements, and generating said image on a display screen based on said decrypted plurality of pixel data elements (Col. 13, lines 49-67 and Col. 14, lines 1-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Narui with the teachings of Shimizu because it would allow to include a non-volatile memory storing an encrypted key with the motivation to safely store personal data of users and to assure safety of highly confidential data shared by the plurality of users (Shimizu, Col. 1, lines 55-60), and to modify the teachings of Narui and Shimizu with the teachings of Muratani because it would allow to include decrypting said encrypted plurality of digital data elements and generating said plurality of pixel data elements based upon said decrypted plurality of digital data elements and generating said image on a display screen based on said decrypted plurality of pixel data elements with the motivation to protect decrypted data transmitted or outputted with being encrypted (Muratani, Col. 1, lines 7-16).

Regarding claim 26, Narui discloses a computer program product for using and storing a cryptography key, comprising:

computer code for receiving a plurality of digital data elements encoded in a display signal wherein said display signal is received according to TMDS format, and wherein said digital data elements represent a plurality of pixel data elements in an encrypted form that represent an image (Col. 2, lines 62-67 and Col. 3, lines 1-67 and Col. 4, lines 30-67).

Narui does not expressly disclose receiving said unencrypted key in said display unit.

However, Shimizu discloses computer code for receiving an unencrypted key computer code for generating said encrypted key from said unencrypted key according to an encryption protocol (i.e., the encrypting device 10 encrypts the transferred temporary key using a master key stored in a master key memory 9), and computer code for generating a decrypted key by decrypting the encrypted key according to said encryption protocol (i.e., the decrypting device 20 decrypts the input data using the master key stored in the master key memory 9, thereby extracting the original temporary key used in encryption)(Col. 7, lines 13-67 and Col. 8, lines 1-20);

computer readable medium for storing the computer code (i.e., storage device 12)(Col. 7, lines 10-27).

Narui or Shimizu does not expressly disclose receiving a display signal in encrypted format.

However, Muratani discloses further comprising computer code for decrypting said encrypted plurality of digital data elements (i.e., scrambled data), generating said plurality of pixel data elements based upon said decrypted plurality of digital data elements, and generating said image on a display screen based on said decrypted plurality of pixel data elements (Col. 13, lines 49-67 and Col. 14, lines 1-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Narui with the teachings of Shimizu because it would allow to include a non-volatile memory storing an encrypted key with the motivation to safely store personal data of users and to assure safety of highly confidential data shared by the plurality of users (Shimizu, Col. 1, lines 55-60), and to modify the teachings of Narui and Shimizu with the teachings of Muratani because it would allow to include computer code for decrypting said encrypted plurality of digital data elements, generating said plurality of pixel data elements based upon said decrypted plurality of digital data elements, and generating said image on a display screen based on said decrypted plurality of pixel data elements with the motivation to protect decrypted data transmitted or outputted with being encrypted (Muratani, Col. 1, lines 7-16).

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narui et al., (U.S. Patent No. 6,313,813 and Narui hereinafter) and Shimizu et al., (U.S. Patent No. 6,085,623 and Shimizu hereinafter), in view of Ashe, (U.S. Patent No. 6,014,745

and Ashe hereinafter), in further view of Philips Semiconductors: The I2C-Buss Specification, Version 2.1, Document Order No. 9398 393 40011.

The teachings of Narui, Shimizu, and Ashe have been discussed before.

Regarding claim 10, Narui, Shimizu, or Ashe does not expressly disclose wherein said path is implemented using I2C protocol.

However, Klein discloses wherein said path is implemented using I2C protocol (Col. 29, lines 8-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu and Ashe with the teachings of Klein to include I2C protocol to send and receive various security commands with the motivation to provide for a simple fault diagnosis and debugging to trace malfunctions immediately (Philips Semiconductors: The I2C Bus Specification, Page 4).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
June 15, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100